I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

It's Personal: Privacy Concerns Associated With Personal Health Records

KRISTEN CARL*

Abstract: Medical records arguably contain a person's most sensitive and private information. Because many medical conditions are hereditary, a single medical record may include equally sensitive information about countless other individuals. The damaging effects brought on by a breach in the security of this information are endless. Third parties – employers, bankers, neighbors – could use this information to discriminate against and potentially ostracize an individual diagnosed with an "unpopular" disease or condition. With the development and rising popularity of the online "personal health record" through mediums such as Google Health and Microsoft HealthVault, two important questions arise: (1) is storing medical information online safe and securely protected; and, (2) in the event of a breach, whom does the law hold accountable?

This article first examines the concept and features of the personal health record ("PHR") and discusses how PHRs differ from other forms of medical records. The second part of this article analyzes the effects a privacy breach would have on the patient and the healthcare provider under the two most pertinent federal laws on PHRs: the Health Insurance Portability and Accountability Act ("HIPAA") and the American Recovery and Reinvestment Act ("ARRA"). In conclusion, this article considers the future of the PHR and the various reforms that have been proposed throughout the literature.

* Kristen Carl is a J.D. candidate at The Ohio State University Moritz College of Law. Carl received a B.A. from Denison University in 2007 in Political Science and Psychology.

I. THE PERSONAL HEALTH RECORD

Until recently, there has not been a uniform definition of a "personal health record" ("PHR"). PHRs are generally understood to be "electronically accessible records of patient health care information that can be maintained by the patient . . . [and] may include medical histories, prescription histories, and lab results that patients can give to their providers."[1] In recent legislation, Congress has defined a PHR as "an electronic record of PHR identifiable health information . . . on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[2]

Essentially, a patient may authorize his or her healthcare provider(s) to upload the patient's medical information to an online source. Although what steps the patient may then take with the information varies from one online source to another, the premise or purpose of the PHR is to grant the patient greater access and control over his or her personal medical information, history, and records.[3] PHRs also provide patients the ability to transmit their medical information to any doctor or hospital, track the progression of illnesses, and maintain personal wellness programs.[4] Common features among the online source or vendor sites, such as Google Health and Microsoft HealthVault, allow the patient to view details of his or her medical history, including prescriptions the patient is currently taking, the name of the doctor under which the patient sought treatment, and when the patient is due for an appointment.[5]

The PHR is part of a broader group of technologies known as "Health Information Technology" ("HIT"). The goal of HIT is to disseminate and direct health information "for use by consumers,

---

[1] DANIEL R. LEVINSON, DEP'T OF HEALTH AND HUMAN SERVICES, OEI-02-06-00270, STATE MEDICAID AGENCIES' INITIATIVES ON HEALTH INFORMATION TECHNOLOGY AND HEALTH INFORMATION EXCHANGE (AUG. 2007), at 2.

[2] American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, § 13400(11), 123 Stat. 115, 259 (2009) (codified as amended at 42 U.S.C. § 17921); Health Breach Notification Rule, 74 Fed. Reg. 42,962, 42,967 (Aug. 25, 2009) (to be codified at 7 C.F.R. pt. 318) (defining PHR in a substantially identical fashion).

[3] Melissa Goldstein & David Blumenthal, *Building an Information Technology Infrastructure*, 36 J. L. MED. & ETHICS 709, 710 (2008).

[4] Bob Brown, *The Number of Online Personal Health Records is Growing, But is the Data in These Records Adequately Protected?*, 3 J. HEALTH CARE COMPLIANCE 35, 35 (2007).

[5] Goldstein & Blumenthal, *supra* note 3, at 710.

providers, payers, [and] insurers."[6] In addition to the PHR, another component of HIT is the "Electronic Health Record" ("EHR"). The EHR functions to store patient data electronically, make that information available to providers on request, allow physicians to enter patient care orders, and present health professionals with standard options for making health care decisions about individual patients.[7] Although commonly confused with the PHR, the distinguishing feature between the two technologies rests with the locus of control. Whereas the patient controls the PHR, the provider controls the EHR. Healthcare providers use the EHR as an "electronic repository," or storage facility, of clinical information gathered by the provider during the patient's course of treatment and care.[8] Typically, access to the EHR is granted only to nurses, doctors, and members of the healthcare provider that own the system.[9]

A. THE ADVANTAGES OF PATIENT HEALTH RECORDS

Advancing HIT has become of great importance in recent years. In 2004, President Bush signed an Executive Order that created the position of the National Coordinator for Health Information Technology.[10] President Bush sought to create a HIT system in which EHRs are the default medical record.[11] With the government paying an estimated 45.9% of the health care expenses,[12] there is great incentive to maximize efficiency and reduce costs. Broad implementation of EHRs is predicted to decrease medical errors, costs, delays, and duplication of tests while improving quality of

---

[6] Goldstein & Blumenthal, *supra* note 3, at 709.

[7] D. Blumenthal & J.P. Glaser, *Information Technology Comes to Medicine*, 356 NEW ENG. J. MED. 2527, 2528 (2007).

[8] Brown, *supra* note 4, at 35.

[9] *Id.*

[10] Exec. Order No. 13,335, 69 Fed. Reg. 24059, 24059 (April 30, 2004); *see also* News Release, U.S. Dep't of Health & Human Services, HHS Secretary and Leading U.S. Companies Say Health Information Technology Should Be Urgent Priority (May 11, 2005), http://www.hhs.gov/news/press/2005pres/20050511.html.

[11] June Sullivan, *Recent Developments and Future Trends in Electronic Medical and Personal Health Records*, THE HEALTH LAWYER, Jan. 2007, at 16, 16.

[12] *Id.*

care.[13] Having a record of a patient's medical history is not helpful if a patient or physician cannot read the hand-written notes, if a page is lost, or if a patient loses part of the file in the midst of changing physicians. Interestingly, one study found that hospitals using EHRs reduced patient mortality rates.[14] Though error in data entry is inevitable with EHRs, the likelihood for confusing patients, their charts, and records is expected to be lower when physicians are not relying on someone else's script and loose-leaf papers.[15] Moreover, electronic records allow for cross-communication and seamless transfer of information when referring or transferring patients from one provider to the next, or even to another department within a hospital.[16]

Likewise, a thoroughly developed PHR system stands to offer abundant benefits. One advantage afforded a patient is convenient access at the click of a mouse to any or all of his or her medical information across providers.[17] Some PHRs are specifically designed to store information that is not typically stored in an EHR, such as "prescription doses and expirations, doctors' instructions, important contact information, family histories, future appointments, and living wills."[18] These types of information can be much more subjective than the information given to a physician, as they may be specifically adapted to the patient's wishes and needs. Those who use Microsoft's HealthVault System through the Mayo Clinic can receive personalized recommendations to undergo additional treatments or tests (*e.g.*, schedule a mammogram) based on characteristics they provide, such

---

[13] *See* News Release, U.S. Dep't of Health & Human Services, OIG Issues Report on State Medicaid Agencies' Initiatives on Health Information Technology and Health Information Exchange (Aug. 21, 2007), http://oig.hhs.gov/publications/docs/press/2007/MedicaidHITRelease.pdf.

[14] Rob Waters, *Computerized Health Records Lower Deaths and Cost, Study Finds,* BLOOMBERG NEWS, January 27, 2009, *available at* http://www.bloomberg.com/apps/news?pid=20601103&sid=aO_Nonz7joYE&refer=us.

[15] *See e.g.,* Sullivan, *supra* note 11.

[16] *See e.g.,* Sullivan, *supra* note 11, at 16.

[17] Sullivan, *supra* note 11, at 19.

[18] Lauren Whetzel, *Medical Records Software Provides Security,* THE WASHINGTON TIMES, May 4, 2009, *available at* http://washingtontimes.com/news/2009/may/04/securing-medical-records.

as family medical history, gender, age, and other health problems.[19] On the provider's side, this translates into information mobility without cumbersome paper files, ensuring "efficient communication and continuity of care."[20] Moreover, patients benefit from improvements in the quality of care at a lower cost.[21] One study found that PHRs could save approximately $19 billion each year.[22]

B. CONCERNS ABOUT PATIENT HEALTH RECORDS

Sobering concerns counter the advantages to adopting new health technologies. Naturally, the concern from the healthcare provider in implementing the new HIT is feasibility. It takes time, personnel, and funding to not only transfer medical records to an online form but also to ensure the provider is well-equipped to handle such an undertaking.[23] Moreover, the provider is also concerned about ensuring that the patient's medical information is adequately protected through ample privacy measures. But what happens when hospitals or doctors close their doors? Patients are similarly concerned about the safety of their personal information, especially the disposal of patient records. For example, a medical doctor in Massachusetts abandoned hundreds of medical records after closing his practice, leaving state officials to question the proper ownership of the records.[24]

---

[19] *Mayo Clinic Backs New Personal Health Record Site*, USA TODAY, Apr. 21, 2009, *available at* http://www.usatoday.com/news/health/2009-04-21-mayo-clinic-health-records_N.htm.

[20] Steve Lohr, *A Hospital is Offering Digital Records*, THE NEW YORK TIMES, Apr. 5, 2009, *available at* http://www.nytimes.com/2009/04/06/technology/companies/06health.html.

[21] Sullivan, *supra* note 17, at 19.

[22] David C. Kaelber et al., Center for Information Technology Leadership, The Value of Personal Health Records (2008), *available at* http://www.citl.org/research/PHR.asp, at 3; *See also Study Predicts Big Savings from PHRs*, HEALTH DATA MANAGEMENT MAGAZINE, Jan. 2009, at 14, 14.

[23] *See* Mayo Clinic Backs New Personal Health Record Site, *supra* note 19.

[24] Kay Lazar, *Patients' Files Poised at Trash Bin*, THE BOSTON GLOBE, Apr. 2, 2009, *available at* http://www.boston.com/news/local/massachusetts/articles/2009/04/02/patients_files_poised_at_trash_bin.

Some hospitals have fired and disciplined employees after discovering they had inappropriately accessed patients' hospital records.[25] In one case, employees accessed medical records of celebrities Farrah Fawcett and Nadya Suleman (a.k.a. "Octomom"), and, in Fawcett's case, sold them to paparazzi.[26] In another case, hackers breached the Commonwealth of Virginia's web site, used by pharmacists to track prescription drug abuse, and deleted over eight million patient records from the site.[27] The hackers placed a ransom note on the homepage asking ten million dollars for the return of the records.[28]

The status of PHRs under HIPPA[29] also raises important concerns. Under HIPAA, a health care provider such as a hospital, doctor's office, or other organization implementing an EHR is considered a "covered entity," which means that it must comply with the privacy and security standards set forth in the law.[30] Thus, the entity must protect patients' medical information in accordance with the federal

---

[25] Kim Zetter, *New Law Floods California with Medical Data Breach Reports*, WIRED, Jul. 9, 2009, *available at* http://www.wired.com/threatlevel/2009/07/health-breaches.

[26] *Id.*

[27] Brian Krebs, *Hackers Break into Virginia Health Professions Database, Demand Ransom*, THE WASHINGTON POST, May 4, 2009, *available at* http://voices.washingtonpost.com/securityfix/2009/05/hackers_break_into_virginia_he.html.

[28] *Id.*

[29] Health Insurance Portability & Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scatter sections of 18, 26, 29, and 42 U.S.C.).

[30] *See* Dennis McMahon, *The Future of Privacy in a Unified National Health Information Infrastructure*, 38 SETON HALL L. REV. 787, 799-800 (2008) ("HIPAA privacy regulations apply to all types of 'individually identifiable health information' in both electronic and paper form. Individually identifiable information includes information that is created or received by a covered entity and is related to the physical or mental condition of an individual, the 'provision of health care to an individual,' or the payment for health care. The information must either identify an individual or be reasonably traceable to an individual . . . HIPAA attempts to safeguard privacy by regulating the circumstances under which individually identifiable information may be used and transmitted. HIPAA allows covered entities to disclose protected health information, without the individual's authorization, to the individual, or for treatment, payment, and healthcare operations. For other disclosures, authorization by the individual is required. Disclosures requiring authorization include disclosures for marketing purpose, disclosure to an employer, and fundraising . . . in the event of a disclosure, the covered entity must also reasonably limit the information disclosed to the minimum amount necessary.").

security standards set forth by HIPAA. These standards allow "protected health information" to pass freely between covered entities but prevent the covered entities from using the information in any way that goes beyond the minimum necessary to implement health care treatment, payment, or health plan "operations."[31] Sharing the information in other ways requires advance written authorization from the individual.[32]

PHRs may not benefit from these protections. The mediums through which many patients store, edit, and upload their medical information (*e.g.,* Google Health) are not considered "covered entities" by HIPAA, and therefore do not have to comply with such minimal (or any) privacy standards.[33] If, however, an EHR is directly uploaded to a PHR vendor site, or if a PHR contains patient health information that was directly extracted from a healthcare provider's EHR on the patient, then that information is considered "personal health information" and disclosure of this information is thought to be subject to HIPAA.[34] This reflects a significant gap in the privacy and security of patient medical information. Much of the information in PHRs, as opposed to that in EHRs, is sensitive in nature and may

---

[31] 45 C.F.R. §§ 164.502(b), 164.514(d); *see also* McMahon, *supra* note 30, at 800-01. (The HIPAA Security Rule mandates that covered entities implement safeguards to protect individually identifiable information transmitted or maintained electronically. "The Security Rule is based on four general requirements with which covered entities must comply: (1) to maintain confidentiality, integrity, and availability in their electronic health information, (2) to protect the data against reasonably anticipated threats to its security or integrity, (3) to prevent impermissible use or disclosure of the information, and (4) to ensure employee compliance with the Security Rule. The Security Rule also requires covered entities to carry out assessments of their compliance with the rule, and to designate a security official to manage employee access to health information. A covered entity must be prepared to deal with a security breach and limit its effects. Finally, the Security Rule establishes both physical and technical safeguards to prevent unauthorized access to protected health information. Many of these physical and technical safeguards, however, are addressable and can be waived under various circumstances." For certain uses and disclosures of information, the Final Privacy Rule (HHS's regulations pertaining to covered entities that include "health plans," "health care clearinghouses," "health care provider," and "hybrid entities") requires notice to patients.).

[32] 45 C.F.R. § 164.508; *see also* McMahon, *supra* note 30, at 799-800.

[33] Brown, *supra* note 4, at 36.

[34] *Id.* at 65 ("Health and Human Services has yet to provide specific guidance on how disclosures of information from the EHR of a covered entity to the PHR of a non-covered entity should be handled with respect to HIPAA . . . ").

extend beyond what is just relayed by the patient to the doctor.[35] It is vital that this information be adequately protected.

Unfortunately, the consequence of escaping privacy obligations under HIPAA is that the online sources where patients upload their information all have very different policies on their privacy rules.[36] One study commissioned by Health and Human Services (conducted by The Altarum Institute) looked at the privacy policies for thirty different online vendors of PHRs and found "wide variation in understanding and implementation."[37] Moreover, the study concluded that many privacy policies were incomplete, there was little consensus on the requirements for what a PHR privacy policy should include, and the data disposal rules and regulations were ill-defined.[38] In particular, only three of the thirty PHR vendors relayed what would happen in the event the vendor closed down or a consumer canceled an account.[39]

Another cause for concern has been the suggestion that if the transfer of personal health information from the covered entity's EHR to the non-covered entity's PHR is "considered a disclosure to carry out treatment, payment, or health care operations, then no authorization from the individual is required to disclose" the personal health information ("PHI").[40] However, HIPAA may mitigate this concern to some extent. Under HIPAA, the non-covered entity must sign a business associate's agreement in which it agrees not to use or disclose the personal health information it receives from the covered entity in a way that would violate the HIPAA Rule.[41]

If the transfer of personal health information from the covered entity's EHR to the non-covered entity's PHR is for any use or

---

[35] *Id.* at 36.

[36] *Id.*, citing R. Lecker et al., The Altarum Institute, Review of the Personal Health Record (PHR) Service Provider Market, Jan. 5, 2007, *available at* http://www.patientprivacyrights.org/site/DocServer/PHRs_Altarum_2007.pdf?.

[37] Lecker, *supra* note 36, at 17.

[38] *Id.*

[39] Policy Briefing, Center for Democracy and Technology, Personal Health Records Need a Comprehensive and Consistent Privacy and Security Framework (Jun. 9, 2009), http://www.mail-archive.com/cdt-announcements@cdt.org/msg00612.html.

[40] Brown, *supra* note 4, at 65.

[41] 45 C.F.R. §§ 164.502(e), 164.504(e); *see also* Brown, *supra* note 4, at 65.

disclosure that is *not* for treatment, payment, or health care operations, greater protections apply.[42] The covered entity must acquire written authorization for the disclosure of personal health information to the PHR vendor.[43] The provisions covering the requirements of a valid authorization apply (*i.e.* they must be in plain language, and contain specifics regarding the information disclosed or used, the person disclosing and receiving the information, expiration, and the right to revoke in writing, etc.).[44]

Furthermore, if the transfer of personal health information from the covered entity's EHR to the non-covered entity's PHR is thought to be a disclosure of personal health information, then the transfer (disclosure) is allowed only at the request of the individual.[45] Any transfers of personal health information from a covered entity to a PHR vendor not covered by the HIPAA rules that were not in compliance with one of the above outlined requirements of the HIPAA privacy rule would constitute a HIPAA violation.[46]

The uncertain nature of accountability in the event of a breach under the federal laws is especially disconcerting because the number of hands that a medical record passes through increases the opportunity for identity theft.[47] Without harmonizing the privacy obligations for password protections and disclosure requirements, health care fraud may, in fact, spread. The protections at the state level are not much help. California was the first state to pass a breach notification law in 2003.[48] California required an "as soon as possible" notification timeline, a private right of action, and no exemptions for encrypted publicly available government data that

---

[42] 45 C.F.R. § 164.508.

[43] 45 C.F.R. § 164.508; *see also* Brown, *supra* note 4, at 65.

[44] Brown, *supra* note 4, at 65; *see also* U.S. Dep't of Health & Human Services, Summary of the HIPAA Privacy Rule (May 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[45] Brown, *supra* note 4, at 65.

[46] *Id.*

[47] Sullivan, *supra* note 11, at 16-17.

[48] Kim Zetter, *Do Breach Notification Laws Work?*, WIRED, Mar. 9, 2009, http://www.wired.com/threatlevel/2009/03/experts-debate.

becomes lost.[49] To date, forty-four states have passed data breach notification requirements, but only three have statutes that explicitly apply to health data.[50] States face the challenges of obtaining funding, sustainability, accurately linking patient data, and dealing with privacy and confidentiality issues."[51]

II. PHRS AND THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009

The 2009 stimulus package, more formally known as the American Recovery and Reinvestment Act of 2009 ("ARRA"), acknowledges the privacy concerns related to PHRs. It makes the most significant changes to federal health care privacy law since the promulgation of HIPAA. This section outlines how the ARRA changes HIPAA and the ways in which these changes seek to protect PHRs.

The ARRA acknowledges that PHI is passed, stored, and communicated with sources outside of covered entities, and is therefore unprotected. Included in the ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH imposes federal breach notification requirements on HIPAA's covered entities and business associates when an unauthorized party obtains "unsecured" personal health information. The ARRA ensures that the entities that are not covered entities under HIPAA are subject to similar breach notification requirements under the Federal Trade Commission's ("FTC") Proposed Rule.

A. HEALTH AND HUMAN SERVICES GUIDANCE

HITECH requires that the Department of Health and Human Services ("HHS") issue interim final regulations for HIPAA covered entities and business associates to provide notification when

---

[49] Scott Berinato, *CSO Disclosure Series, Data Breach Notification Laws, State by State* (Feb. 12, 2008), http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State.

[50] Letter from Center for Democracy & Technology to Donald Clark, Sec'y of U.S. Fed. Trade Comm'n, Health Breach Notification Rulemaking (Jun. 1, 2009), at 13-14, http://www.cdt.org/healthprivacy/20090601_ftc_breach_comments.pdf.

[51] Goldstein, *supra* note 3, at 713.

"unsecured"[52] PHI in any form[53] is breached.[54] Following a breach, a covered entity must "notify each individual whose unsecured personal health information has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed in the breach."[55] Business associates must "notify the covered entity of the breach and identify for the covered entity the individuals whose unsecured personal health information has been, or reasonably believed to have been, breached."[56] The notifications must be made "without unreasonable delay" and no later than sixty days after discovery of the breach.[57]

If the breach of unsecured personal health information affects more than 500 residents of a particular state, then notice must be given to prominent media outlets within that state.[58] Also, for breaches affecting more than 500 individuals, notice must be given to the Secretary of State.[59] Finally, the Secretary must post on the HHS website a list of the covered entities involved in the breach of

---

[52] DEP'T OF HEALTH & HUMAN SERVICES, HHS GUIDANCE SPECIFYING THE TECHNOLOGIES AND METHODOLOGIES THAT RENDER PROTECTED HEALTH INFORMATION UNUSABLE, UNREADABLE, OR INDECIPHERABLE TO UNAUTHORIZED INDIVIDUALS FOR PURPOSES OF THE BREACH NOTIFICATION REQUIREMENTS UNDER SECTION 13402 OF TITLE XIII (HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT) OF THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009; REQUEST FOR INFORMATION (2009), at 2, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf (defining "unsecured protected health information" as "protected health information that is not secured through the use of a technology or methodology . . . that render[s] protected health information unusable, unreadable, or indecipherable to unauthorized individuals").

[53] HHS Guidance, *supra* note 52, at 12 ("Data in motion" (i.e. data moving through wireless network); "data at rest" (i.e. data that is in a file); "data in use" (i.e. data that is being created, maintained, etc); or "data disposed" (i.e. data that's been discarded).).

[54] American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, § 13402(a), 123 Stat. 115, 260 (2009) (codified as amended at 42 U.S.C. § 17932(a)).

[55] *Id.; see also* HHS Guidance, *supra* note 52, at 7.

[56] American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, § 13402(b), 123 Stat. 115, 260 (2009) (codified as amended at 42 U.S.C. § 17932(b)); *see also* HHS Guidance, *supra* note 52, at 7.

[57] HHS Guidance, *supra* note 52, at 7.

[58] HHS Guidance, *supra* note 52, at 8.

[59] *Id.*

unsecured personal health information of more than 500 individuals.[60]

When a covered entity notifies an individual directly affected by a breach of their protected health information, the notification must include:

> (1) a description of what happened, including the date of the breach and the date of the discovery of the breach; (2) a description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code); (3) the steps an individual should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.[61]

The HHS Guidance specifies two methods to make personal health information unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction. "Encryption" occurs where there is "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" as defined in HIPAA's Security Rule.[62] "Destruction" of the media on which personal health information is collected may occur when (1) "paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed" or (2) "electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved."[63]

---

[60] *Id.*

[61] *Id.*

[62] 45 C.F.R. § 164.304.

[63] HHS Guidance, *supra* note 52, at 17.

HIPPA's covered entities and business associates are not required to adhere to the HHS guidelines for ensuring the protected health information is properly de-identified.[64] If they choose to follow the guidelines, however, their actions will fall under a safe harbor, which prevents them from having to provide notification in the event of a breach.[65]

With respect to vendors of PHRs and other non-HIPAA covered entities, these vendors or entities must notify the FTC in the event of a security breach of health records.[66]

B. THE FEDERAL TRADE COMMISSION HEALTH BREACH NOTIFICATION RULE

As part of the ARRA, the FTC issued a proposed Health Breach Notification Rule on April 16, 2009. Where the HHS Guidelines applied to HIPAA covered entities and business associates, the FTC's Rule only concerns venders of PHRs, PHR related entities, and third-party service providers that are not HIPAA covered entities and business associates.[67]

After a PHR vendor discovers[68] a breach of security of unsecured[69] PHR identifiable health information in the vendor's, or related entity's, PHR the vendor must notify each affected individual whose information was compromised and notify the FTC.[70] Third-party service providers[71] must provide notice of the breach to a senior

---

[64] *Id.* at 10.

[65] *Id.* at 10-11.

[66] *Id.* at 5-6.

[67] Federal Trade Commission, Health Breach Notification Rule, 16 C.F.R. § 318.1 (2009).

[68] A breach is considered to be "discovered" the "first day on which such breach is known to a vendor of personal health records, PHR related entity, or third-party service provider . . . or should reasonably have been known to such vendor of personal health records . . . to have occurred." 16 C.F.R. § 318.3(c) (2009).

[69] The FTC adopts HHS's definition of "unsecured" as stated in its Guidelines. *See* Ctr. for Democracy & Tech., *supra* note 48.

[70] 16 C.F. R. § 318.3(a)(1) (2009).

[71] Defined as "an entity that: (1) provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and (2)

official at the PHR vendor, or a related entity, to which it provides services.[72] This notification must identify the affected individuals whose information was, or is reasonably believed to have been, breached.[73]

Generally, notifications of these breaches must be made "without unreasonable delay" and never later than 60 calendar days after the discovery of a security breach.[74] The burden of proving that the notifications satisfied the requirements rests upon the PHR vendors, related entities, or third-party service providers.[75] Prompt notification may be made via first-class mail or electronic mail, if the individual provides express affirmative consent.[76] Notice by way of telephone may be made in addition to the notification via mail or e-mail.[77] If ten or more individuals cannot be reached by these notification means, then notification shall be made by a conspicuous posting on the vendor's or related entity's home page of its website for ninety days, or in the print and broadcast media where the affected individuals reside.[78] Accompanying these notices must be a toll-free phone number that individuals can call to learn whether their information was breached.[79]

Prominent media outlets in the relevant areas must also be notified if 500 or more residents of the relevant state or jurisdiction had, or are reasonably believed to have had, their PHR identifiable health information acquired.[80] The FTC must be notified of the breach and if the breach involved 500 or more individuals, then notice

---

accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services." 16 C.F.R. § 318.2(h) (2009).

[72] 16 C.F.R. § 318.3(b).

[73] *Id.*

[74] 16 C.F.R. § 318.4(a).

[75] 16 C.F.R. § 318.4(b).

[76] 16 C.F.R. § 318.5(a)(1).

[77] 16 C.F.R. § 318.5(a)(3).

[78] 16 C.F.R. § 318.5(a)(2)(i).

[79] 16 C.F.R. § 318.5(a)(2)(ii).

[80] 16 C.F.R. § 318.5(b).

must occur no later than ten business days after the breach was discovered.[81] If less than 500 individuals were affected, the PHR vendor or related entities may, instead of giving immediate notice, maintain a log of breaches and submit it to the FTC each year.[82]

Notification of the breach must include: (1) a brief description of how the breach happened; (2) the date of the breach; (3) the date of the discovery of the breach; (4) a description of the types of unsecured information that was acquired (*e.g.*, full name, Social Security number, date of birth, home address, account number); (5) steps individuals should take to prevent further harm from the breach; (6) a brief description of what the PHR vendor or related entity is doing to investigate, mitigate losses, and protect against further breaches; and (7) contact procedures (*e.g.*, toll-free telephone number, e-mail address, website, or postal address) for individuals to ask questions or receive information.[83]

While the FTC acknowledges that, at times, it will be difficult to determine whether a breach took place, the Rule creates a presumption that unauthorized acquisitions will "include unauthorized access to unsecured PHR identifiable health information" unless the PHR vendor, related entity, or third-party service provider "has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition of such information."[84]

Recently, the FTC issued charges against CVS Caremark for failing to take "reasonable and appropriate security measures to protect the sensitive financial and medical information of its customers and employees."[85] The FTC's complaint alleged that CVS Caremark did not utilize reasonable policies and procedures for the disposal of secure personal information, failed to properly train employees, did not apply reasonable measures to assess compliance for disposing of personal information, and did not practice a reasonable process for

---

[81] 16 C.F.R. § 318.5(c).

[82] *Id.*

[83] 16 C.F.R. § 318.6 (2009).

[84] 16 C.F.R. § 318.2(a).

[85] Press Release, FTC, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009), http://www.ftc.gov/opa/2009/02/cvs.shtm.

discovering and remedying risks to personal information.[86] Despite CVS Caremark's claim that it "wants you to know that nothing is more central to our operations than maintaining the privacy of your health information," they violated the FTC Act, which forbids unfair and deceptive practices.[87]

The Department of Health and Human Services also alleged charges against CVS Caremark regarding HIPAA privacy violations due to its improper disposal of personal medical information.[88] Consequently, CVS Caremark had to pay $2.25 million and "implement a robust corrective action plan that requires Privacy Rule compliant policies and procedures for safeguarding patient information during disposal, employee training and employee sanctions for noncompliance."[89]

C. ARRA STRENGTHENS AND CHANGES HIPAA

While over forty-five states currently have security breach notification laws, only a few include notification requirements if health information is compromised.[90] However, the ARRA broadens the scope of notification obligations for any entity dealing with health information, regardless of whether it falls under HIPAA.[91] The ARRA preempts any contrary state law in the same manner that HIPAA

---

[86] *Id.*

[87] *Id.*; As a result of CVS Caremark violating the FTC Act, the consent order requires CVS to "establish, implement, and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of the personal information it collects from consumers and employees." CVS must also "obtain, every two years for the next 20 years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order."

[88] Press Release, Dept. of Health and Human Serv., CVS Pays $2.25 Million and Toughens Practices to Settle HIPAA Privacy Case (Feb. 18, 2009), http://www.hhs.gov/news/press/2009pres/02/20090218a.html.

[89] *Id.*

[90] Health Breach Notification Rulemaking, *supra* note 50, at 13.

[91] American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, 123 Stat. 115, § 13402 (2009) (hereinafter "ARRA").

does.[92] However, if a state law is more stringent regarding security breach notification obligations, the state law will remain effective.[93]

The ARRA also amends the HIPAA Privacy and Security Rules, thereby influencing both HIPAA-covered entities and business associates.[94] HIPAA's Privacy and Security rules are national standards that ensure that electronic health information and data are stored, transmitted, and disclosed through protected and safe means. Beginning in 2010, the ARRA will subject business associates to several of the health information protection obligations that the Privacy and Security Rules currently require for covered entities.[95] Furthermore, the ARRA requires that vendors have business associate agreements with covered entities.[96] Business associates will be obligated to implement the Security Rule's safeguards, and must use and disclose protected health information only as directed by the Privacy Rule.[97] Business associates will be subject to civil and criminal penalties if they violate these security provisions. HIPAA only extends liability to business associates by virtue of their business associate agreements with covered entities.[98] The ARRA stipulates that if a covered entity fails to cure a material breach under its business associate agreement, the business associate must terminate the agreement or, if termination is not possible, notify HHS of the uncured breach.[99] Finally, any new requirements that the ARRA imposes on business associates must be incorporated into business associate agreements by February 17, 2010.[100]

---

[92] *Id.* at § 13421.

[93] *Id.*

[94] *Id.* at § 13401.

[95] *Id.*

[96] *Id.*

[97] *Id.* at §§ 13401(a), 13405(a).

[98] *Id.* at § 13404(a).

[99] *Id.* at § 13402(e)(3).

[100] *Id.* at § 13423.

The ARRA further requires that, in order for a covered entity to be compliant with the "minimum necessary" standard[101] with respect to the use, disclosure, or request of protected health information, a covered entity must limit such protected health information to a limited data set to the extent practicable.[102] A limited data set is comprised of protected health information from which personal identifiers are removed.[103]

For entities that use or maintain EHRs, the ARRA eliminates the exception under the HIPAA Privacy Rule that allows covered entities to exclude from their accounting to individuals disclosures of protected health information related to treatment, payment, and health care operations.[104] Thus, a health care provider, insurer, or any other covered entity using EHRs will be subject to much more extensive reporting requirements, because these disclosures quite possibly make up the majority of covered entities' disclosures.

The ARRA also imparts a significant new burden on certain business associates regarding accounting for disclosures. A covered entities has the option to either directly account for disclosures of business associates acting on its behalf, or it can give a list of business associates that the individual requesting an accounting may contact so that the business associate must report its own disclosures of protected health information.[105]

The ARRA supplements the Privacy Rule's current provisions detailing when an authorization is required for disclosures of protected health information by prohibiting the sale of protected health information in particular circumstances unless a covered entity acquires a valid authorization that includes "a specification of whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information."[106]

---

[101] 45 C.F.R. § 164.514(d)(3)(ii)(A) (i.e. a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.).

[102] ARRA, § 13405(a)(1)(A).

[103] 45 C.F.R. § 164.514(e)(2).

[104] ARRA, § 13405(c)(1)(A).

[105] *Id.* at § 13405(c)(3).

[106] *Id.* at § 13405(d)(1).

The ARRA also makes changes to the current practices regarding marketing under the Privacy Rule. Specifically, the ARRA narrows restrictions on the use of protected health information for marketing purposes. Current exceptions to the marketing rule (*e.g.*, permitting communications encouraging purchase or use of products or services in connection with treatment or with case management or care coordination)[107] are not allowed if a covered entity is paid to make the communication.[108] However, this is allowed if the marketing communication merely describes a currently prescribed drug or biologic for an individual and payment for such communication is a reasonable amount; a covered entity obtains a written authorization from an individual; or a business associate makes the communication consistent with the business associate agreement between it and a covered entity.[109]

The ARRA strengthens penalties for non-compliance with HIPAA by increasing civil monetary penalties according to the level of a particular violator's intent. It also enhances HIPAA enforcement mechanisms by authorizing state attorneys general to enforce violations of the HIPAA Privacy and Security Rules against covered entities, as well as business associates under determined circumstances.[110]

By making the biggest changes to HIPAA since the law was enacted in 1996, the ARRA stands to make a dramatic impact on the privacy rules regulating personal health records. Section III will discuss the future of personal health records in light of the ARRA.

III. THE FUTURE OF PHRS

A little over a week before the ARRA was signed into law, CNN political pundit Campbell Brown demonstrated the need for greater privacy measures for medical records.[111] Over the course of two

---

[107] 45 C.F.R. § 164.501.

[108] ARRA, § 13406(a)(2).

[109] *Id.*

[110] *Id.* at § 13410.

[111] *Campbell Brown: No Bias, No Bull* (CNN television show broadcast Feb. 6, 2009), *available at* http://transcripts.cnn.com/TRANSCRIPTS/0902/06/ec.01.html; *see also Campbell Brown: No Bias, No Bull* (CNN television broadcast Feb. 10, 2009), *available at* http://transcripts.cnn.com/TRANSCRIPTS/0902/10/ec.01.html.

shows, she had Senior Medical Correspondent Elizabeth Cohen attempt to access CNN National Correspondent Gary Tuchman's medical information over the internet. With just a social security number and date of birth, she was able to access health insurance claims in which every doctor's appointment was listed for the past eighteen months for not only Gary, but for his entire family.[112] Cohen also found her own information available on her health insurance company's website.[113] Cohen's doctor's appointment and all the doctor's appointments and lab tests for her husband and four children were listed.[114] As a preventative measure, Cohen suggested going to any pharmacy, hospital, or insurance company that would have this information online and creating an account using a safe username and password, and setting up security questions and answers.[115] In spite of the alarming results of Cohen's experiment, she was quick to highlight the advantages of electronic medical records:

> . . . I once did a story with a gentleman who had a CAT scan. And the doctor called him and said your CAT scan looks fine. You don't have any problems. Well, because these records were online, the patient went on and read his own CAT scan report. He wasn't fine. They found a spot on his thyroid. He had thyroid cancer and his doctor completely missed it. The patient caught it only because his records were online. And that hospital that that gentleman uses, they have a much more secure site than the insurance company that we've been talking about.[116]

Transitioning to online medical records clearly enables personal control over one's health and medical information. The key is to prevent privacy invasions.

One article has suggested a "Cyber-Patients Bill of Rights" in which a "framework of principles intended to provide a foundation for

---

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Campbell Brown: No Bias, No Bull* (CNN television broadcast Feb. 10, 2009), *available at* http://transcripts.cnn.com/TRANSCRIPTS/0902/10/ec.01.html.

much-needed legislation or a meaningful self-regulatory system" is outlined. The eight "rights" include the: (1) Right to an Effective Architecture of Privacy; (2) Right to Informed Consent; (3) Right to Control Disclosure of Information; (4) Right to Transparency; (5) Right to Accessibility and Portability; (6) Right to Due Process and Dispute Resolution; (7) Right to Heightened Protection for Minors; and (8) Right to Anonymity.[117] The Right to an Effective Architecture of Privacy mandates that health networking providers must offer the latest technological resources to protect user information from being used, accessed, or divulged in an unwarranted manner, which requires continual updating of privacy-protection technology and applications in a commercially reasonable fashion.[118]

The Right to Informed Consent is the right to be educated before disclosing personal information online.[119] Patients must have access to information regarding the technological medium and its capabilities, the website's privacy policies, and who has access to cyber-patient records, postings, and online activities.[120] The Right to Control Disclosure of Information calls for patients to have the right to control their information by determining what information is private on a context-by-context basis with the ability to grant or deny access.[121] The Right to Transparency is the right to know exactly how personal information is used, collected, and accessed.[122] It also includes knowing who else has access to it and the ability of the individual to inspect and modify their information and to obtain records of disclosures and authorizations.[123] The Right to Accessibility and Portability includes the right to access, alter, and delete any information pertaining to them, including the right to transfer their profiles to another online health network.[124] The Right to Due Process

---

[117] Patricia Sanchez Abril & Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights*, NW. J. TECH. & INTELL. 244, 270-75 (2008).

[118] *Id.* at 270-71.

[119] *Id.* at 271.

[120] *Id.*

[121] *Id.* at 272.

[122] *Id.*

[123] *Id.*

[124] *Id.* at 273.

and Dispute Resolution includes the right to be notified of, defend, and appeal any allegation or charge of conduct that could result in the removal of information from the website or loss of information contained there, as well as the right to have access to a trusted forum for dispute resolution.[125] The Right to Heightened Protection for Minors includes the right for minors to a heightened level of privacy protection on each of the above Rights.[126] Finally, the Right to Anonymity includes the right to communicate anonymously, subject to certain limitations.[127]

IV. CONCLUSION

In light of the recent passage of the ARRA, it will be interesting to see how the statute, in application, will fill in the gaps left over from HIPAA and possibly eliminate the need for a "cyber-patient bill of rights." Declaring that citizens want strong privacy and security laws governing their personal health information is seemingly an understatement. Yet, are breach notifications the solution? Flooding mailboxes or inboxes with notifications may cause consumers to grow numb and ignore the information.[128]

What *is* known is that the passage of the ARRA marks a significant progress in protecting patient medical information through PHRs, while enabling the health care industry to develop progressive health information technologies.

---

[125] *Id.* at 274.

[126] *Id.*

[127] *Id.* at 275.

[128] Kim Zetter, *Do Breach Notification Laws Work?*, WIRED, Mar. 9, 2009, http://www.wired.com/threatlevel/2009/03/experts-debate.